IN THE CLAIMS:

Please amend the claims as follows.

1. (Currently amended) A method of passing configuration information between a DHCP server and a DHCP client, the method comprising:

forming a DHCP message having a vendor-specific portion including at least one parameter representing configuration information encoded as a triplet comprising a code field, a length field, and a value field, wherein said code field includes an indication of encryption of the value field, and said value field comprises a set of one or more name-value pairs encrypted in accordance with the code field; and

storing said at least one parameter of the vendor-specific portion of the DHCP message in a repository on the DHCP server;

transmitting the DHCP message including the vendor-specific portion from the DHCP server to the DHCP client;

editing said at least one parameter on the DHCP client; and

writing the edited at least one parameter from the DHCP client into the repository for storage on the DHCP server.

2. (Original)   The method of claim 1, wherein the value field of said triplet comprises a single name-value pair.

3. (Original)   The method of claim 1, wherein the code field is used to define the form of encryption of the value field.

4. (Original)   The method of claim 3, wherein the code field is used to identify the encryption algorithm used for the value field.

5. (Original)   The method of claim 3, wherein the code field is used to identify the key length used in the encryption of the value field.

6. (Original)   The method of claim 1, wherein at least one parameter included within the vendor specific portion is encrypted, and at least one other parameter included within the vendor specific portion is not encrypted.

7. (Original)   The method of claim 1, wherein said at least one parameter is not formally defined within DHCP.

8. (Original)   The method of claim 1, wherein said encryption is performed using a key specific to the DHCP client.

9. (Original)   The method of claim 8, further comprising the client initially transmitting said specific key to the DHCP server.

10-11. (Cancelled)

12. (Currently amended) The method of claim [[11]]1, further comprising replicating the stored at least one parameter in the repository on the DHCP server for use by one or more other DHCP clients.

13. (Currently amended) A dynamic host configuration protocol (DHCP) server comprising:
    a store containing DHCP information for at least one DHCP client, said DHCP information including a vendor-specific portion containing at least one parameter representing configuration information for the DHCP client encoded within a triplet comprising a code field, a length field, and a value field, wherein said code field includes an indication of encryption of the value field, and said value field comprises a set of one or more name-value pairs encrypted in accordance with the code field; and
    a network interface operable to transmit a DHCP message including the vendor-specific portion to the DHCP client;

wherein said store comprises a repository on the DHCP server, wherein said repository is configured to store said vendor-specific portion including said at least one parameter;

wherein said network interface is operable to receive an edited version of said at least one parameter from the DHCP client and to write the edited at least one parameter from the DHCP client into the repository for storage on the DHCP server.

14. (Original) The apparatus of claim 13, wherein the value field of said triplet comprises a single name-value pair.

15. (Original) The apparatus of claim 13, wherein the code field is used to define the form of encryption of the value field.

16. (Original) The apparatus of claim 15, wherein the code field is used to identify the encryption algorithm used for the value field.

17. (Original) The apparatus of claim 15, wherein the code field is used to identify the key length used in the encryption of the value field.

18. (Original) The apparatus of claim 13, wherein at least one parameter included within the vendor specific portion is encrypted, and at least one other parameter included within the vendor specific portion is not encrypted.

19. (Original) The apparatus of claim 13, wherein said at least one parameter is not formally defined within DHCP.

20. (Original) The apparatus of claim 13, wherein said encryption is performed using a key specific to the DHCP client.

21. (Original) The apparatus of claim 20, wherein the specific key is initially received from the DHCP client via said network interface.

22-23. (Cancelled)

24. (Currently amended) The apparatus of claim [[23]]13, wherein the stored at least one parameter in the repository may be is replicated on the DHCP server for use by other DHCP clients.

25. (Cancelled)

26. (Currently amended) A method of managing a DHCP server having a repository of DHCP client configuration data, the method comprising:

receiving vendor-specific data representing configuration data for said client, wherein said vendor-specific data comprises at least one triplet of a code field, a length field, and a value field, wherein said code field includes an indication of encryption of the value field, and said value field comprises a set of one or more name-value pairs encrypted in accordance with the code field; and

storing in the repository the received vendor-specific configuration data for the client in the repository on the DHCP server;

transmitting said vendor-specific configuration data from the DHCP server to a DHCP client;

receiving an edited version of said vendor-specific configuration data from the DHCP client and writing the edited version of said vendor-specific configuration data from the DHCP client into the repository for storage on the DHCP server.

27-28. (Cancelled)

29-52. (Cancelled)

53. (New) A method of passing configuration information between a DHCP server and a DHCP client, the method comprising:

forming a DHCP message having a vendor-specific portion including at least one parameter representing configuration information encoded as a triplet comprising a code field, a length field, and a value field, wherein said code field includes an indication of encryption of the value field, and said value field comprises a set of one or more name-value pairs encrypted in accordance with the code field;

storing said at least one parameter of the vendor-specific portion of the DHCP message in a repository on the DHCP server;

transmitting the DHCP message including the vendor-specific portion from the DHCP server to the DHCP client; and

replicating the stored at least one parameter in the repository on the DHCP server for use by one or more other DHCP clients.

54. (New) A dynamic host configuration protocol (DHCP) server comprising:

a store containing DHCP information for at least one DHCP client, said DHCP information including a vendor-specific portion containing at least one parameter representing configuration information for the DHCP client encoded within a triplet comprising a code field, a length field, and a value field, wherein said code field includes an indication of encryption of the value field, and said value field comprises a set of one or more name-value pairs encrypted in accordance with the code field; and

a network interface operable to transmit a DHCP message including the vendor-specific portion to the DHCP client;

wherein said store comprises a repository on the DHCP server, wherein said repository is configured to store said vendor-specific portion including said at least one parameter;

wherein the stored at least one parameter is replicated on the DHCP server for use by other DHCP clients.